Amendments to the Claims

1. (currently amended) A method of processing network security protocol data packets, ~~comprising:~~

~~providing a cryptography processing architecture on a chip;~~

~~passing~~ receiving, in a chip, a packet including non-pre-padded network security protocol data for both authentication and cryptography operations from [[a]] an off-chip processor ~~source to said chip~~ over a peripheral communications bus;

conducting [[,]] ~~in hardware~~ [[,]] authentication and encryption [[,]] operations on the network security protocol data of said packet; and

passing [[the]] said crypto-processed ~~network security protocol data~~ packet from said chip to said off-chip processor ~~source~~;

wherein said authentication and encryption for the packet is performed within said chip ~~non-pre-padded network security protocol data is passed between said chip and said source~~ in a single pass.

2. (original) The method of claim 1, wherein said network security protocol is SSL (v3).

3. (original) The method of claim 1, wherein said network security protocol is TLS.

4. (currently amended) The method of clam 1, further comprising simultaneously with conducting the cryptography operations on the network security

protocol data pre-loading network security protocol data from a second non-pre-padded network security protocol packet onto the chip.

5. (currently amended) The method of claim 4, further comprising simultaneously with conducting the encryption operations on the network security protocol data of the first packet, conducting, in hardware, authentication operations on the network security protocol data from the second network security protocol packet.

6. (original) The method of claim 1, wherein said conducting, in hardware, authentication and encryption operations on the non-pre-padded network security protocol data comprises conducting padding and alignment operations on the chip.

7. (currently amended) The method of claim 6, wherein a calculation of a pad length for padding operations is conducted by a pad engine ~~component of the chip architecture~~.

8. (original) The method of claim 1, wherein said conducting, in hardware, authentication and encryption operations on the network security protocol data comprises feeding back a MAC value calculated during authentication operations for processing in the encryption operations.

9. (original) The method of claim 1, wherein said encryption operations further include decryption operations.

10. (original) The method of claim 9, wherein conducting, in hardware, ~~authentication and decryption operations on the network security protocol data comprises~~ feeding back decryption data for processing in the authentication operations.

11-25. (canceled)

26. (currently amended) A method of processing network security protocol data packets, comprising:

receiving, at a chip, a packet including non-pre-padded network security protocol data for both authentication and cryptography operations from [[a]] an off-chip processor ~~source to said chip~~ over a peripheral communications bus;

aligning, at the chip, the receiving non-pre-padded network security protocol data to provide aligned network security protocol data;

conducting, at the chip, authentication operations and at least one of encryption operations and decryption operations on the aligned network security protocol data of said packet to provide processed network security protocol data; and

passing the processed network security protocol data in a packet from the chip to said off-chip processor ~~the source~~;

wherein said authentication and encryption for the packet is performed within said chip ~~the non-pre-padded network security protocol data is passed between the chip and the source~~ in a single pass.

27. (previously presented) The method of claim 26 comprising removing non-valid data from the received non-pre-padded network security protocol data.

28. (previously presented) The method of claim 26 comprising packing the received non-pre-padded network security protocol data.

29. (previously presented) The method of claim 26 comprising storing the aligned network security protocol data in a FIFO to accumulate a predefined amount of data before commencing the authentication operations and the at least one of encryption operations and decryption operations.

30. (previously presented) The method of claim 29 wherein the predefined amount of data comprises 512 bits.

31. (previously presented) The method of claim 26 wherein the authentication operations comprise authenticating at least a portion of the aligned network security protocol data.

32. (previously presented) The method of claim 31 where the at least a portion of the aligned network security protocol data comprises Content Type, Length and Data that is aligned into rows of data where each row of data contains a single type of data.

33. (previously presented) The method of claim 31 comprising aligning, for encryption operations, at least a portion of the received non-pre-padded network security protocol data and the authenticated at least a portion of the aligned network security protocol data to provide the aligned network security protocol data for the encryption operations.

34. (previously presented) The method of claim 33 wherein aligning, for encryption operations, comprises removing non-valid data.

35. (previously presented) The method of claim 33 wherein aligning, for encryption operations, comprises adding padding.

36. (previously presented) The method of claim 26 comprising storing the aligned network security protocol data for the encryption operations in a FIFO to accumulate a predefined amount of data before commencing the encryption operations.

37. (previously presented) The method of claim 26 wherein aligning comprising aligning, within a decryption path, the received non-pre-padded network security protocol data to provide the aligned network security protocol data for the decryption operations.

38. (previously presented) The method of claim 37 comprising:

decrypting the aligned network security protocol data for the decryption operations; and

providing at least a portion of the decrypted data for the authentication operations.

39. (previously presented) The method of claim 38 comprising aligning the at least a portion of the decrypted data for the authentication operations.

40. (previously presented) The method of claim 26 comprising performing at least a portion of the authentication operations and at least a portion of the at least one of encryption operations and decryption operations in parallel.

41. (previously presented) The method of claim 1 comprising aligning and padding the non-pre-padded network security protocol data on the chip to enable the non-pre-padded network security protocol data to be passed in a single pass.

42. (cancel).

43. (previously presented) The method of claim 1 comprising receiving all SSL packet portion by the chip, padding and aligning the packet portions, cryptographically processing the packet portions and outputting the cryptographically processed packet portions from the chip in a single pass over a data bus.

44. (currently amended) The method of claim 1 wherein:

the authentication operations are performed by an authentication component of the ~~chip~~;

the encryption operations are performed by an encryption component of the chip; and

authentication data generated by the authentication component is passed to the encryption component and aligned by the encryption component.

45. (currently amended) The method of claim 1 wherein:

the authentication operations are performed by an authentication component of the chip;

the encryption operations are performed by an encryption component of the chip; and

decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component.